PETIT ABC DE CRYPTOGRAPHIE


```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.0.6 (MingW32) - GPGOE 0.4.1
Comment: For info see http://www.gnupg.org

hQGOA0nQC0jB079qEAX8CpeYFWwy6ckEZggVnL68AjILgPa0mxiejGvYUBvfb2pJ
HQnq6o07Hmx5ix0TvDeyh8nhhNy+92z+y/CbBxY4D8xVC/knpBq6n5OhdeMONteV
SbDVOhjPHPqkUta0Jy//xss7GMGRMFpRhnfKne/+K2V2xYN7+V9IC4zYWj5SQ/im
5dyW89KdBQNUOM5WCL3L0IdT3kSIz6MjyuOABtxlUXK6Bag27YVTE9L4DdzuZ0A6
zGwTH89Yy10xrAybtG+cTDfq0jDxO+ZVwZqGjE6eoz4ZKA6OkWTKruLs3WQ7pqVB
ovIxFSpOBpjS+cFERQXyvWUsgbP2heYFNJPgnnWcPbdqaKC1EJsgYyYM4yl5AZQ3
t8bcRixMmtT015uR4HHgxsHXVDJ2xHIpZLylAQh3JwkcaTq0XrerhZy1XUhcEKUz
iWdtN+TlaEAZzdu4cJdGP0fZcj9VMHYsBBCLZ48N4n4nzePuEiMQQt1C4FpQ7kBY
hhmcBC1IjafNGc8Zs9jKpP0DOFdvzpyyPrXuHCu6lvGRb4rYZ7NFWTIqkl3hCBds
9ELOYO6Ncb7MgOwgkqnj2dAleUxNET3AyXCI5xA86EYsZZZjTXjVJOgu6sVBwJHU
ron2IO1eHYnqlIs3X/XOivwmB5bAo61ksC9SEG24mft3uHjb9ahC6Kwd5OK45MMD
L07DQba8UCxq66kEXmDID4ZaEdC1tdCYt1b0AsMx/nV9a3widirMsOrraaJJCQAJ
DJqoCzEzyF7UB9q5aEN1JroJ7MWvsFO4kwU1/qv3lqfyw3N+yM6kjf0apRy5K1eM
j4Nb12I5CAx0jGMTBnx5bEJqcwk0iv99YAYGdtFT+sf6Haehl4hVPlXkYLFyv+7h
2DZbMczWNTh9T8qOdny+7zeyY71Ks1vgzMz8mZF95dZyxNr75xJkFctHlyL83env
bvaJxYWpDzMAnDbyexnRWv96iKp/Ml/LtiQS3dzE1gud8lN9pQPGcD1N64px837i
g9d+pT7vH9gWsuMPJRBhPmXw70erINcSYn0y5XCeqFJfZfi6+fDZrxqqxTQY0rfK
oVG4/xpLIs+y5/Jzd6YcJQBltGP//Qy8+Dkmm6FM2hMStFMgnOzvGmg=
=Kj9b
-----END PGP MESSAGE-----
```


nov. 2002 - Lausanne

Cryptons nos mails!

Pourquoi la crypto?

Lorsque tu envoies un mail, il est possible qu'un appareil, appelé un sniffeur et programmé uniquement pour "pomper" des infos qui passent sur internet, ait comme tâche de prendre une copie de tous tes mails. Quel indiscrétion, n'est-ce pas? Et pourtant, faire cela est techniquement très facile à mettre en oeuvre. Tout les systèmes de protections (par ex. mot de passe pour ouvrir un fichier) proposés par les gros éditeurs de logiciels sont conçus pour être aisément contournés par des services étatiques et autres...

Mais que faire, alors, au secours! :-)

Avec la cryptographie, tu pourras protéger tes communications électroniques. Par contre, ton message est stocké en "clair" sur ton ordinateur, car lorsque tu tapes un texte, l'ordinateur en garde toujours une trace. Donc si tu subis une perquisition, ton fichier est retrouvable...

Il ne faut pas oublier les restrictions de la cryptographie des mails: il n'efface pas tes fichiers temporaires, ou ne crypte pas les données de ton disque dur! D'autres outils existent pour cela...

Bien des militantEs affirment que crypter ses mails est pire que tout puisque on attirera l'attention des systèmes de surveillance... ce qui est faux, il suffit de s'imaginer que l'état, l'armée, les banques, le e-commerce... ne se gênent pas d'utiliser cette technique.

Est-ce vraiment inviolable? Non, les messages cryptés peuvent être décryptés. Par contre, il est plus ou moins facile de le faire. Cela dépend beaucoup des précautions que tu vas prendre dans l'utilisation de la cryptographie. Il faut savoir qu'en utilisant aujourd'hui les meilleurs algorithmes de cryptographie, il faudrait attendre des "super ordinateurs cryptoniques au magma d'enfer" (prévu dans 70 ans environ) et qu'il leur faudrait encore beaucoup de temps pour arriver à bout de ta clé. Des moyens beaucoup plus simples existent: le vol, la torture, la surveillance électronique (des caméras sont capable de savoir ce tu tapes sur ton clavier à plus de 100m), la perquisition, et surtout ton inattention! En résumé des moyens très simples pour certaines instances...

Assez de discours! Et en pratique???

De façon résumée.

1- créer sa paire de clé: la publique et la privée, la première à distribuer.
2- échanger par mail ou sur disquette sa clé publique avec ses “camarades”.
3- vérifier la clé publique du correspondant avec l’empreinte.
3- crypter son premier message, et l’envoyer.
4- décrypter la réponse avec sa clé privée.

Une paire de clé peut avoir deux usages principaux: crypter tes communications électroniques et/ou protéger les fichiers de ton disque dur en les cryptant.

Avec quel programme cryptons-nous nos messages?

Le type de programme le mieux adapté pour crypter ses données serait un programme qui ne soit pas écrit pas une agence gouvernementale, qui ait été testé par des personnes à travers le monde, qui soit libre et dont nous ayons le code source afin de vérifier son intégrité. Et bien, ça existe! C’est GnuPG, abrégé GPG. Un autre programme existe: PGP (Pretty Good Privacy). PGP appartient à une entreprise, il n’est donc pas libre. Par contre, ses propriétaires ont dernièrement publié les sources du programmes. Nous n’utiliserons pas ce programme pour des problèmes idéologiques (c’est un produit commercial), et pour des problèmes de confiance.
Malheureusement, GPG fonctionne en mode commande, ce qui signifie que chaque commande doit être entrée en tapant un texte. Pour les néophytes, l’utilisation est rendue assez difficile. Nous utiliserons donc des interfaces graphiques, ainsi notre souris nous suffira pour crypter nos messages. Pour windoze, le programme est WinPT-GPG; sous linux, il s’appelle kgpg ou gpa, et sous MacOS, MacGPG.

A l’action!

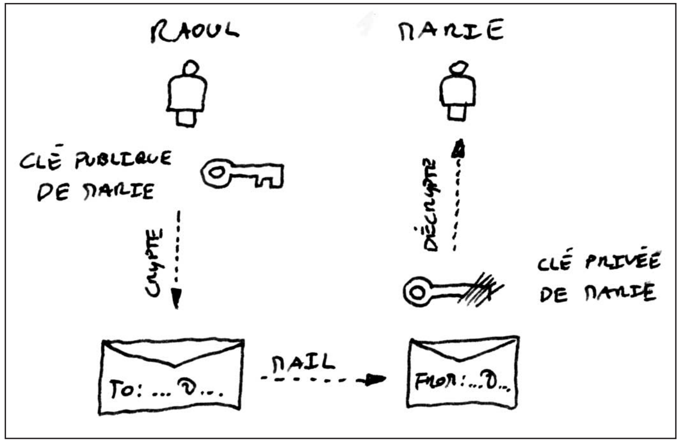


fig. 1: cryptage d’un message

La cryptographie à clé publique est très simple une fois son concept compris. Imaginons deux correspondantEs: Raoul veut envoyer un message à Marie (voir fig.1). Ils se sont déjà échangé leurs clés publiques. Selon le schéma ci-dessous, Raoul va crypter son message avec la clé publique de Marie. Par contre, seul le possédantE de la clé privée , dans ce cas-ci Marie, pourra l’ouvrir une fois fermé; le message est décrypté grâce à cette clé. Tu devineras donc que la clé privée est un point faible de ce système de cryptographie. La clé privée est donc protégée par un mot de passe. Elle ne doit jamais être possédée par d’autres que toi-même.
Le but de l’amusement? Distribuer notre clé publique à tout le monde, et motiver nos correspondantEs à faire des émules!

Comment distribuer sa clé publique?

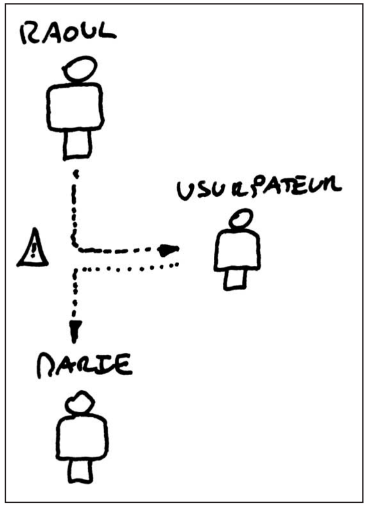


fig. 3: interception d’une clé publique

Il est difficile de donner sa clé publique par écrit ou oralement (voir exemple d’une clé fig. 2). Nous pouvons donc l’échanger par disquette ou cd-rom, le moyen le plus sûr, puisque nous la remettons en main propre à notre correspondantE. Mais le mail est tout de même bien plus pratique... Nous pouvons donc l’envoyer par mail dans un fichier attaché ou dans le message même. Il existe aussi des serveurs de clé publique sur lesquels tu peux publier ta clé. Gros problème de l’échange de clé par voie électronique: comment être certain que le destinataire

est la personne en qui nous avons confiance? Quelqu'unE peut très bien intercepter le message (voir fig. 3), et substituer ta clé publique par la sienne, pour ensuite pouvoir décrypter très facilement tous tes messages! Ainsi, si A envoit un message à B, alors que C a intercepté l'échange de clé, C va décrypter le message envoyé par A, en prendre connaissance, le crypter et le renvoyer à B, sans que B ni A ne se rendent comptent de rien! (voir le schéma ci-dessous). Il est donc important de vérifier l'empreinte (fingerprint) de sa clé, et ceci par un moyen direct (rencontre physique, téléphone, ...).

Comment créer une paire de clé (privée et publique)?

Afin de créer des clés, différents types d'algorithmes peuvent être utilisés, mais nous nous contenterons ici d'utiliser celui proposé par défaut par GPG: DSA & Elgamal. Le monde des algorithmes, de la confiance que l'on peut leur accorder est complexe...

- se choisir une taille pour sa clé: par défaut, GPG propose 1024 bits, pour une sécurité normale, jusqu'à aujourd'hui inviolée. En choissant une taille de 2048 bits, tu seras mieux protégé, mais le cryptage/décryptage sera un peu ralenti.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
...
mQGiBD3vhp0RBACo/XPazgzU4ZlylE6LG0E9D/
uGBKUIUfcz0wYJ2ELlwo6qoRUV=Lf6j
...
-----END PGP PUBLIC KEY BLOCK-----
```

fig. 2: exemple d'une clé publique

- GPG te demande ensuite la date d'expiration de ta paire de clés. Comme tout système de protection, plus le temps passe, plus le risque que ta clé ait été compromise est grand. Il est donc conseillé de changer de clef de temps en temps. Tu peux donc choisir la date à partir de laquelle la clef sera expirée, c'est à dire qu'il ne sera plus possible de l'utiliser pour crypter des messages. Une durée d'un an semble raisonnable dans la plupart des cas.
- Après cela, GPG te demande la nom de la clé et l'adresse mail à laquelle la clé sera liée. Important: chaque clé est "attachée" à une adresse mail.
- Enfin, afin de protéger ta clé privée, tu dois entrer un mot de passe long. Si quelqu'un a accès à ton ordinateur, seul ce mot de passe l'empêchera de déchiffrer tes messages. D'où son importance. Ton mot de passe long (jusqu'à un nombre de caractère illimité, et n'importe lesquels) ne doit pas être impossible à mémoriser (ne jamais l'écrire), mais s'il est trop simple, il est inutile. Veille à ne pas introduire des mots du dictionnaire, qu'elle qu'en soit la langue, car ceux-ci sont très facilement devinables. Mélange lettres, chiffres, et caractères spéciaux (tel que |, {, [, #, ...), majuscules, minuscules. Ton mot de passe doit être long, au minimum 10 caractères. N'insére aucun espace.

Signer des clés publiques

Lorsque tu as reçu la clé publique de ton/ta correspondantE, l'idéal est de vérifier son empreinte (fingerprint) par un contact direct (téléphone ou courrier postal). L'empreinte est unique. Si elle correspond, alors tu peux signer la clé publique.
La clé publique est utilisable même si tu ne la signes pas, mais peut-être que d'autres l'ont interceptée... et tu ne peux pas le savoir! De même, certains programmes n'acceptent pas d'utiliser une clé publique qui n'est pas signée. Mais ne signe pas une clé si tu ne l'as pas vérifiée.

Déchiffrer et chiffrer des documents et des textes.

Enfin, nous y arrivons! Tu peux autant crypter du texte que des fichiers. Dans la cas où tu aimerais protéger des fichiers de ton disque dur, il est préférable de les crypter avec une autre paire de clé que celle utilisée pour tes correspondances. Les menus changent d'un programme à l'autre, d'une interface graphique à une autre. Très souvent, tu as deux possibilités:

1) tu tapes ton texte, tu l'enregistres dans un fichier, tu le cryptes, et tu l'envoies tel quel.

2) tu utilises le copier/coller: tu sélectionnes ton texte, tu le copies (souvent Ctrl+C), tu cryptes le presse-papier, puis tu colles ton texte crypté dans un nouveau fichier, ou dans ton mail.

Facile, non?

Crypter des fichiers?

GPG te permet de crypter des fichiers, mais il faut savoir qu'il existe des systèmes plus performants qui cryptent l'entier de ton disque dur ou tout un dossier par exemple. Si tu veux crypter un fichier avec GPG, crée de préférence une autre clé privé que celle utilisée pour ton mail.

Approfondissement

Beaucoup de spécificités n'ont pas été abordées ici sur GPG, dont la toile de confiance, l'effacement de son identité d'un message crypté, les attaques possibles sur les données cryptées. Les sites référencés ci-après pourront t'aider.

FAQ (en construction...)

Référence:

www.gnupg.org - excellente documentation, plein d'info, de manuel, etc...
www.bugbrother.com - site qui fourmille d'info sur la sécurité en général
www.opengpg.fr.st - beaucoup d'infos, de plugin's
www.squat.net/print - vas-y et découvre le projet!
macgpg.sourceforge.net - pour le programme mac
www.winpt.org - pour le programme windoze